West Science Law and Human Rights
Vol. 3, No. 04, October 2025, pp. 459~469

Analysis of Criminal Liability for Personal Data Violations: Case Studies of the General Elections Commission and E-Commerce from the Perspective of the ITE Law and the PDP Law 2023–2024

Ilmi Firdaus Aliyah[1], Novandi Dwi Putra[2]
[1,2] Universitas Mayjen Sungkono,

Article Info

Article history:

Received Oct, 2025
Revised Oct, 2025
Accepted Oct, 2025

Keywords:

Personal Data Protection Law, ITE Law, criminal liability, data breach, normative juridical analysis

ABSTRACT

This study examines criminal liability for personal data violations in Indonesia through a normative juridical analysis of case studies involving the General Elections Commission (KPU) and e-commerce platforms during the 2023–2024 period. The research focuses on the intersection between the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law) to determine how these regulations govern the protection of personal data and the imposition of criminal sanctions. Findings reveal that while the ITE Law provides a legal foundation for addressing electronic crimes, it lacks specificity in handling cases of institutional negligence and corporate responsibility. In contrast, the PDP Law introduces comprehensive provisions, including criminal sanctions for both intentional and negligent violations, but faces enforcement challenges due to limited institutional capacity and overlapping jurisdictions. Analysis of the KPU and e-commerce data breaches shows weak legal enforcement, lack of accountability, and insufficient public awareness. The study concludes that effective personal data protection in Indonesia requires legal harmonization between the ITE and PDP Laws, establishment of a dedicated supervisory authority, and enhancement of institutional and public capacity to ensure compliance and accountability.

Corresponding Author:

Name: Ilmi Firdaus Aliyah
Institution Universitas Mayjen Sungkono
e-mail: ilmifirdausa@gmail.com

1. INTRODUCTION

The digital transformation has reshaped the ways personal data is collected, stored, and processed across online transactions, e-government platforms, and social media interactions. However, this rapid shift also increases the risks of data breaches and misuse, particularly when institutions fail to implement adequate security measures. In Indonesia, major data leak incidents involving the General Elections Commission (KPU) and e-commerce platforms such as Tokopedia and Bukalapak during 2023–2024 have exposed significant weaknesses in the national data protection framework. These incidents raised widespread public concern regarding the security and integrity of citizens' personal information. Although Indonesia's regulatory regime has been strengthened through the Personal Data Protection Law (PDP Law) of 2022 and the Electronic Information and Transactions Law (ITE Law), challenges persist in legal harmonization, regulatory dualism, institutional coordination, and enforcement capacity [1], [2], [3]. The situation is further complicated by low levels of public digital literacy and limited institutional readiness, which hinder effective monitoring and compliance with data protection obligations [4], [5].

The exposure of voter data from KPU and consumer information from Tokopedia and Bukalapak demonstrates the scale of potential harm caused by weak cybersecurity systems and insufficient legal enforcement, raising critical questions about the criminal liability of data controllers, processors, and responsible institutions. The implementation of both the PDP Law and ITE Law is constrained by unclear jurisdiction, regulatory inconsistencies, and the absence of a robust independent supervisory authority, making it difficult to ensure accountability and effective data governance [1], [4]. Accordingly, key recommendations include harmonizing the PDP and ITE Laws to eliminate regulatory overlaps, strengthening digital infrastructure, enhancing institutional capacity, providing education and training for business actors, and improving public awareness to safeguard digital rights more effectively [2], [5]. Strengthening these legal and institutional mechanisms is therefore essential to ensure comprehensive and resilient personal data protection

The enactment of Indonesia's Personal Data Protection (PDP) Law represents a major step in strengthening digital governance, as it provides a dedicated legal framework for safeguarding personal data and introduces explicit criminal sanctions for violations. By contrast, the Electronic Information and Transactions (ITE) Law—initially intended to regulate electronic information and transactions more broadly—has been widely used to prosecute cyber-related offenses such as unauthorized access and data manipulation, yet it lacks detailed mechanisms for personal data protection. This regulatory gap has created ambiguities in how both laws interact, particularly regarding overlapping jurisdiction, the classification of offenses as administrative or criminal, and inconsistencies in enforcement. Scholars note that the general nature of the ITE Law contributes to regulatory dualism with the PDP Law [1], while the PDP Law, although inspired by international standards like the GDPR, still faces challenges in implementation due to institutional overlap and normative inconsistencies [1], [6]. Recent data breach cases from 2023–2024 further illustrate these issues, revealing the complexities of determining criminal liability within an evolving legal landscape.

These overlapping frameworks also complicate the enforcement of liability for personal data violations, which may involve both individuals and institutions under provisions that prohibit misuse, including doxing [7]. Effective implementation requires harmonization between the PDP and ITE Laws as well as stronger institutional capacity to handle data protection issues [1], [5]. Case studies from recent breaches highlight deficiencies in existing enforcement mechanisms, emphasizing the need for clearer legal consequences and more accessible reparations for victims [6], [7], [8]From a legal standpoint, addressing these challenges requires a deeper analysis of substantive and procedural elements—such as determining who can be held responsible, the circumstances under which liability arises, and the scope of sanctions—to ensure that Indonesia's data protection regime is able to effectively respond to incidents and safeguard citizens' digital rights.

This study employs a normative juridical analysis to examine the legal foundations, statutory interpretations, and doctrinal perspectives surrounding personal data protection and criminal liability, using the KPU and major e-commerce breach cases as focal points to assess whether Indonesia's current legal framework effectively deters violations and ensures accountability while maintaining consistency between the ITE Law and PDP Law in regulating data security and imposing criminal sanctions. Ultimately, this paper contributes to the broader discourse on digital governance and legal reform by arguing that effective personal data protection requires legal harmonization, stronger institutional coordination, and improved public awareness. The findings aim to provide valuable insights for policymakers, law enforcers, and scholars in developing a more coherent, enforceable, and equitable approach to data protection that balances individual rights, institutional responsibilities, and technological realities within Indonesia's rapidly evolving digital ecosystem.

2. LITERATURE REVIEW

2.1 The Concept of Personal Data Protection

The protection of personal data in Indonesia, as established under Law No. 27 of 2022 (PDP Law), constitutes a crucial legal and ethical framework for safeguarding individual privacy and aligns with international standards such as the European Union's GDPR, incorporating principles of lawfulness, fairness, transparency, and accountability; however, its implementation faces significant challenges due to limited procedural detail and institutional readiness compared with the GDPR's more developed mechanisms, including mandatory Data Protection Impact Assessments (DPIAs) and independent supervisory authorities [4], [9]. While the GDPR's extraterritorial scope and strong enforcement illustrate the importance of enhancing Indonesia's regulatory capacity [4], obstacles in applying the PDP Law persist, particularly the absence of a dedicated supervisory institution, insufficient public and institutional awareness, complex data processing structures, and weak security systems, alongside external threats such as data interception in government and financial sectors [9], [10], [11]Furthermore, although the PDP Law is grounded in human rights principles—linking personal data protection to constitutional rights to privacy under the 1945 Constitution—rapid technological advancements continue to generate new threats that require stronger statutory enforcement, improved institutional coordination, and resilient data governance frameworks to ensure meaningful protection for citizens in the digital era [10], [12].

2.2 Overview of the Electronic Information and Transactions (ITE) Law

The ITE Law, although not originally designed as a data protection law, contains provisions relevant to data breach cases—such as consent requirements for personal data use and prohibitions on unauthorized access or alteration of electronic information—yet its effectiveness remains limited due to its general nature, vague definitions, and lack of specific enforcement mechanisms, which have resulted in inconsistent court applications and scholarly criticism [1], [13]. These shortcomings have led to growing calls for harmonization with the more comprehensive PDP Law, which provides a systematic and internationally aligned framework for data protection, including explicit criminal penalties for unauthorized data distribution that the ITE Law does not address unless accompanied by other offenses [1], [14]. Implementation challenges further hinder the ITE Law's effectiveness, as multiple interpretations, ambiguous article formulations, and limited cybercrime awareness among law enforcement officers create procedural uncertainty and weaken enforcement outcomes [15], [16].

2.3 *The Personal Data Protection (PDP) Law: Legal Innovations and Challenges*

The Personal Data Protection Law (PDP Law), enacted as Law No. 27 of 2022, marks a major development in Indonesia's legal framework by providing a comprehensive system for managing personal data, defining the roles of data controllers and processors, and imposing administrative as well as criminal sanctions for violations; its key provisions include the requirement for explicit consent before data processing (Articles 20–22), the rights of data subjects to access, correct, and delete their data (Articles 9–13), and the obligation for data controllers to ensure data security (Article 35), alongside criminal penalties such as imprisonment and fines for intentional or negligent misuse of personal data (Articles 67–70) [9], [17]. Despite these advancements, the law faces significant implementation challenges, including the absence of an independent supervisory authority to enforce compliance, potential overlaps and jurisdictional ambiguities with existing regulations like the ITE Law, and structural weaknesses when compared with international standards such as the GDPR, particularly regarding mechanisms like data portability and privacy by design [3], [9], [18]. Research further shows that institutional and enforcement gaps remain substantial, with Putri & Nugroho (2023) emphasizing the uncertainty created by regulatory overlaps and the need for clearer integration of the PDP Law within Indonesia's broader digital governance ecosystem.

2.4 *Criminal Liability in Data Breach Cases*

Criminal liability in Indonesian law regarding personal data violations requires assessing the intent or negligence of data controllers and processors, with the Personal Data Protection (PDP) Law providing a framework to hold both individuals and corporations accountable for breaches, particularly as incidents of data misuse increase and digital evidence becomes more complex; this law emphasizes clear delineation of responsibilities and allows sanctions against corporations for systematic negligence or inadequate security measures, consistent with Article 45 paragraph (1) of the PDP Law. Corporate liability is reinforced through strict liability provisions that hold corporations responsible for misuse committed by individuals within the organization, with possible sanctions including fines of up to 2% of annual revenue, business license revocation, and criminal penalties for corporate officers [19]. At the individual level, mens rea plays a central role in distinguishing intentional from negligent acts, shaping the severity of penalties, although proving criminal intent remains challenging in cybercrime cases due to the diffuse and complex nature of digital evidence [20]. Enforcement further faces obstacles such as weak supervisory mechanisms, low public legal literacy, and inadequate digital infrastructure, with cases like the Bjorka hacking incident illustrating the need for both penal and non-penal strategies, including enhanced digital literacy and strengthened cybersecurity systems to ensure effective implementation of data protection norms [21], [22]

2.5. *Theoretical Framework*

This study is grounded in two core legal theories: the Theory of Legal Protection (Teori Perlindungan Hukum) developed by Satjipto Rahardjo, which asserts that law must function to safeguard human dignity and rights—emphasizing the state's obligation to protect individuals' privacy and security in the context of personal data—and the Theory of Criminal Liability (Teori Pertanggungjawaban Pidana), which examines how responsibility is attributed to individuals or institutions based on intentional or negligent acts that violate criminal norms; by applying these theoretical foundations, the study assesses how Indonesian law assigns criminal responsibility for data breaches and evaluates whether existing legal frameworks effectively protect citizens' personal data from misuse or unauthorized exposure.

3 RESEARCH METHODS

3.1 Research Approach

This study employs a normative juridical (doctrinal) research approach that focuses on examining legal norms, statutory provisions, doctrines, and principles governing personal data protection and criminal liability, emphasizing legal reasoning rather than empirical data collection; as stated by Soerjono Soekanto (2006), normative legal research aims to identify in concreto the application and consistency of laws in resolving legal issues, and in this study it is used to analyze the legal relationship between the ITE Law and the PDP Law in addressing personal data breaches, interpret relevant provisions on criminal sanctions, liability, and institutional responsibility, and evaluate the implementation and enforcement of these laws in the 2023–2024 data breach cases involving public and private entities, thereby enabling an assessment of how effectively Indonesia's legal system ensures justice, deterrence, and protection for citizens whose personal data has been compromised.

3.2 Type of Research

This research adopts a descriptive-analytical approach, aiming to present the factual conditions of data protection enforcement while analyzing them through legal reasoning; the descriptive component outlines how data breaches occurred in the KPU and various e-commerce platforms, including institutional responses and public reactions, whereas the analytical component evaluates these events within the framework of relevant legal provisions to determine whether they fulfill the legal elements of criminal liability as stipulated under the ITE and PDP Laws, thereby providing a comprehensive understanding of both the practical realities and the legal implications of personal data breaches in Indonesia.

3.3 Source of Legal Materials

This study relies on secondary data consisting of primary, secondary, and tertiary legal materials, including primary materials such as the ITE Law (Undang-Undang No. 11 Tahun 2008 as amended by Undang-Undang No. 19 Tahun 2016), the Personal Data Protection Law (Undang-Undang No. 27 Tahun 2022), the 1945 Constitution, relevant government regulations, ministerial decrees, official guidelines on data protection and cybercrime, as well as court decisions and jurisprudence related to personal data breaches; secondary materials comprising legal textbooks, journal articles, policy briefs, academic papers on data protection, cyber law, and criminal liability, publications from institutions such as Kominfo and BSSN, and comparative studies referencing the GDPR and ASEAN data protection frameworks; and tertiary materials in the form of legal dictionaries, encyclopedias, news archives, and credible online sources that provide factual context and support the analysis of the data breach cases examined in this research.

3.4 Data Collection Techniques

Data collection in this study was carried out through documentary research and literature review by systematically identifying, collecting, classifying, and analyzing legal documents and academic sources, including relevant statutes and regulations, scholarly interpretations, journal publications, and policy commentaries, as well as factual information on the KPU and e-commerce data breaches compiled from official press releases, digital forensic reports, and verified media coverage from 2023 to 2024; all materials were then organized thematically to support the legal analysis of criminal responsibility, institutional negligence, and the mechanisms of personal data protection in Indonesia.

3.5 Data Analysis Techniques

This research employs qualitative juridical analysis, focusing on a logical, systematic, and interpretative evaluation of legal norms and principles, using statutory interpretation to examine the provisions, objectives, and constitutional alignment of the ITE and PDP Laws, comparative analysis to identify overlaps and differences between both laws while referencing international benchmarks such as the GDPR for best-practice assessment, and case study analysis to evaluate how the legal framework has been applied in the KPU and e-commerce data breach cases and whether responsible parties can be held criminally liable; the insights generated from these analytical techniques are then synthesized to determine the adequacy of Indonesia's legal response to personal data privacy violations and to assess whether existing regulations effectively ensure accountability and protection for citizens.

4. RESULTS AND DISCUSSION

4.1 Overview of Personal Data Violation Cases in 2023–2024

In 2023, Indonesia's General Elections Commission (KPU) experienced a massive data breach that exposed more than 200 million voter records, including names, national identification numbers (NIK), addresses, and polling information. The leaked data appeared on online forums and was allegedly sold on the dark web, raising major public concern and prompting investigations by the Ministry of Communication and Informatics (Kominfo) and the National Cyber and Crypto Agency (BSSN). Although the KPU claimed that the breach originated from older databases or external sources rather than its main election system, digital forensic assessments suggested critical vulnerabilities such as weak encryption and limited access controls. Despite the gravity of the incident, no clear criminal accountability was established, as authorities focused primarily on mitigation efforts and data recovery rather than pursuing prosecution, revealing a significant gap in the application of the PDP Law's criminal sanctions.

The KPU's assertion that the breach did not come from its main system but from legacy databases reflects a broader and recurring pattern also seen in e-commerce platforms: inadequate cybersecurity architecture. Digital forensic findings have shown that vulnerabilities such as poor encryption, weak authentication protocols, and insufficient access control measures are systemic issues across both election infrastructure and corporate digital ecosystems. Comparative cases illustrate this similarity: failures in election systems, as seen in the Antrim County error caused by operator mistakes and inadequate procedures [23], the rapid compromise of the Washington, D.C. Internet voting trial server [24], and the severe vulnerabilities in New South Wales' iVote system due to insecure external servers [23], mirror the weaknesses that have caused major e-commerce breaches. Tokopedia's leak of 91 million user records due to failures in preventive and post-incident handling [25] and T-Mobile's repeated breaches in 2021 and 2023, which underscored the necessity of zero-trust architectures and granular access control [26], highlight the urgent need for robust cybersecurity protocols across both the public and private sectors.

In parallel with the election-related breach, multiple e-commerce platforms—including Tokopedia, Bukalapak, and Shopee—experienced recurring data leaks between 2023 and 2024. These breaches compromised user account data, passwords, transaction histories, and in certain cases, financial information, with most companies attributing the incidents to third-party vulnerabilities or external hacking attempts. Although such breaches clearly violate the rights to data protection guaranteed under the PDP Law, the legal responses largely consisted of administrative warnings and public apologies rather than criminal prosecution. This pattern indicates a persistent enforcement gap in applying the PDP Law's criminal provisions to private-sector actors, demonstrating that Indonesia's current legal and institutional frameworks remain insufficient to ensure accountability and deter future data privacy violations.

4.2 Legal Analysis Based on the ITE Law

The ITE Law is Indonesia's earliest legal instrument governing electronic information and transactions, containing provisions that address unauthorized access and illegal manipulation of electronic data. Article 30 paragraph (1) stipulates that "any person who intentionally and without authority accesses another person's electronic system" may be subject to imprisonment or fines, while Article 32 paragraph (1) criminalizes altering, deleting, or disseminating electronic information without authorization. In the KPU and e-commerce data breach cases, the actions involving unauthorized access and dissemination clearly fulfill these legal elements, making hackers or other unauthorized actors liable under the ITE Law. However, when breaches stem from institutional negligence—such as weak cybersecurity architecture, insufficient encryption, or poor access control—the effectiveness of the ITE Law diminishes, as it does not explicitly criminalize negligence or systemic failures on the part of institutions.

This limitation reflects a broader structural issue noted by legal experts such as Sinta Dewi (2021), who argue that the ITE Law is primarily oriented toward prosecuting individual cybercrime offenders rather than addressing corporate or institutional irresponsibility. Consequently, while perpetrators who directly infiltrate systems can be prosecuted, organizations that fail to implement adequate safeguards often evade criminal sanctions despite contributing to the conditions that enable breaches. This gap exposes a critical flaw in Indonesia's digital governance framework, demonstrating the need for complementary regulation—such as the PDP Law—to address institutional accountability and ensure a more comprehensive approach to personal data protection.

4.3 Legal Analysis Based on the PDP Law

The Personal Data Protection Law (PDP Law), enacted in 2022, establishes a comprehensive regulatory framework governing data controllers and processors, introducing criminal sanctions for both intentional and negligent acts that result in personal data misuse or unlawful disclosure. Article 67 paragraph (1) stipulates that individuals or institutions who intentionally obtain or disclose personal data illegally may face up to five years of imprisonment and/or fines of up to IDR 5 billion, while Article 70 paragraph (2) extends liability to corporations when violations occur due to inadequate security measures or non-compliance. The law mandates preventive and repressive obligations, requiring robust security systems and transparent data management practice [11], with Articles 67 and 70 emphasizing the criminal and corporate liabilities associated with data breaches [27]. Despite its strong legal structure, the PDP Law's enforcement remains limited, particularly in the absence of clear implementation guidelines and institutional readiness.

Enforcement challenges are further compounded by the absence of a dedicated supervisory authority, a gap that significantly weakens monitoring and sanctioning mechanisms, as evidenced in the KPU breach case [11]. Overlapping authority among regulatory bodies—such as Bawaslu and law enforcement—creates procedural uncertainty and erodes public trust [28]. In the KPU incident, the institution, acting as a data controller, had a legal obligation under Article 35 to ensure the confidentiality and security of voter data; however, inadequate organizational and technical measures indicated potential negligence. Yet, due to the non-operational status of the supervisory authority at the time, formal prosecution and administrative sanctions could not be pursued. A similar pattern emerged in the e-commerce sector, where companies acknowledged breaches but criminal liability was not pursued because of difficulties in proving intent (mens rea) and causation (causa proxima), especially when breaches were attributed to external cyberattacks, which complicated direct corporate responsibility assessments.

To strengthen the PDP Law's effectiveness, scholars recommend establishing an independent supervisory authority capable of enforcing compliance, conducting investigations, and issuing sanctions [11]. Clearer regulations and improved coordination among regulatory bodies are also necessary to reduce jurisdictional overlap and enhance public trust [29]. Despite being more advanced than previous regulatory frameworks, the PDP Law still encounters institutional and procedural limitations that hinder full implementation. Putri & Nugroho (2023) emphasize that Indonesia requires a dedicated Data Protection Authority (DPA) to ensure comprehensive, consistent, and enforceable protection of personal data across both public and private sectors.

4.4 Comparative Analysis: ITE Law vs. PDP Law

A comparison between the ITE Law (Law No. 11/2008) and the PDP Law (Law No. 27/2022) shows that the ITE Law broadly regulates electronic transactions and cybercrimes with a focus on intentional acts committed by individuals, imposing imprisonment and fines but lacking a designated supervisory authority, while the PDP Law specifically governs personal data protection, covers both individuals and institutions as data controllers or processors, extends liability to include intentional and negligent acts, and introduces administrative, civil, and criminal sanctions supported by the mandate to establish a Data Protection Authority; in practice, the ITE Law is applied mainly to hackers and direct cybercrime actors, whereas the PDP Law is designed to regulate corporate and institutional responsibility. This comparison demonstrates that although the ITE Law provides a foundational framework for addressing electronic crimes, it lacks the specificity required for robust personal data governance, while the PDP Law offers more detailed obligations and broader liability yet continues to suffer from weak enforcement and limited institutional readiness. Together, the two laws create a dual-layered regulatory system, but without proper harmonization their overlapping provisions generate legal uncertainty, causing law enforcement agencies to hesitate in determining which statute should apply and resulting in frequent under-prosecution of data breach cases.

4.5 Discussion

The findings reveal a significant disconnect between Indonesia's legal norms and actual enforcement practices, showing that although the PDP Law introduces comprehensive protection mechanisms, its effectiveness ultimately depends on the readiness of implementing institutions and the political will to enforce its provisions; this highlights the urgent need for harmonization between the ITE and PDP Laws to eliminate overlapping regulations and ensure consistent application across public and private sectors, alongside the strengthening of institutional capacity through the establishment of an independent Data Protection Authority (DPA) with clear investigative and sanctioning powers. Furthermore, stronger corporate compliance is necessary, requiring e-commerce platforms and digital service providers to adopt higher cybersecurity standards, conduct regular audits, and maintain transparent data management practices in accordance with Article 35 of the PDP Law, while public empowerment initiatives—such as citizen education on data protection rights and reporting mechanisms—must be prioritized to enhance participation in digital governance. Judicial development is equally essential, as courts and prosecutors need specialized training in cyber law and digital forensics to adjudicate data protection cases effectively and uphold fairness in the enforcement of personal data rights.

5. CONCLUSION

The analysis of criminal liability for personal data violations based on the KPU and e-commerce case studies during 2023–2024 reveals substantial legal and institutional weaknesses in Indonesia’s data protection regime. Although both the ITE Law and the PDP Law offer mechanisms for responding to data breaches, the lack of harmonization between them creates ambiguity in enforcement, scope, and jurisdiction. The ITE Law continues to focus on intentional cybercrimes committed by individuals, offering limited tools for addressing institutional or corporate negligence, whereas the PDP Law introduces a more comprehensive regulatory structure governing data controllers and processors and establishes civil, administrative, and criminal sanctions for violations. Despite its stronger framework, the effectiveness of the PDP Law remains constrained by the absence of a fully operational Data Protection Authority (DPA) and weak coordination among enforcement bodies. The KPU case exposes systemic vulnerabilities in public-sector cybersecurity and accountability, while recurring breaches in the e-commerce sector reveal persistent compliance gaps and insufficient consumer protection. Both cases highlight how current enforcement remains largely reactive and mitigation-oriented, providing minimal remedies for victims and failing to establish deterrence.

Therefore, this study concludes that Indonesia must urgently harmonize the ITE and PDP Laws, strengthen institutional capacity, and establish a dedicated supervisory authority capable of overseeing compliance, conducting investigations, and imposing sanctions. Public empowerment through improved digital literacy is equally essential to ensure that citizens understand and can exercise their data protection rights. Effective enforcement of data protection laws also requires technological expertise, enhanced judicial competence in cyber law and digital forensics, and robust inter-agency collaboration to build a trustworthy and resilient digital governance ecosystem. In summary, the future of personal data protection in Indonesia depends not merely on the existence of comprehensive legal frameworks but on the clarity of legal responsibilities, the commitment of both state and private actors, and the consistent and competent enforcement needed to uphold privacy and accountability in the digital era.

REFERENCE

[1] I. M. Kholis, “Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia,” *Staatsr. J. Huk. Kenegaraan dan Polit. Islam*, vol. 4, no. 2, pp. 275–299, 2024.

[2] D. D. Wijayanto and K. W. Indrayanti, “Personal Data Protection in Digital Business Based on the Law on Personal Data Protection,” *Int. J. Res. Soc. Sci. Humanit. ISSN 2582-6220, DOI 10.47505/IJRSS*, vol. 6, no. 8, pp. 6–12, 2025.

[3] I. Lutrianto and R. Riswaldi, “Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia,” *Greenation Int. J. Law Soc. Sci.*, vol. 3, no. 2, pp. 345–350, 2025.

[4] M. Taufiq and A. S. Kenyo, “The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR,” *Int. J. Business, Law, Educ.*, vol. 6, no. 2, pp. 1260–1268, 2025.

[5] F. Nadiah and S. A. Wiraguna, “TINJAUAN HUKUM TERHADAP PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA,” *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 6, pp. 270–278, 2025.

[6] H. Rahmawati, “Aspek Hukum dalam Transaksi Bisnis Digital serta Upaya Perlindungan Data Pribadi Konsumen dalam Era Teknologi,” *JISPENDIORA J. Ilmu Sos. Pendidik. Dan Hum.*, vol. 3, no. 3, pp. 133–141, 2024.

[7] S. M. Hasya, A. M. Abdullah, and R. M. Damarjati, “Aspek Hukum Pertanggungjawaban Pelaku dan Upaya Pemulihan Hak Korban Atas Kejahatan Doxing,” *Eksekusi J. Ilmu Huk. dan Adm. Negara*, vol. 3, no. 1, pp. 176–190, 2025.

[8] R. S. Ahmad, D. A. Puspaningtyas, and M. N. K. Al Ismariy, “PERLINDUNGAN HUKUM TERHADAP PRIVASI DATA PRIBADI DI ERA DIGITAL,” *The Juris*, vol. 9, no. 1, pp. 15–23, 2025.

[9] A. S. Kriswandaru, B. Pratiwi, J. Laksito, W. Ariani, and S. Sholikatun, “Analisis Yuridis terhadap Penggunaan Teknologi Blockchain dalam Pengamanan Data Pribadi: Studi Kasus di Indonesia,” *Perkara J. Ilmu Huk. dan Polit.*, vol. 2, no. 4, pp. 531–540, 2024.

[10] Z. Makkawaru and A. Almusawir, “Perlindungan hukum data pribadi dalam perspektif hak asasi manusia,” *Indones. J. Leg. Law*, vol. 7, no. 1, pp. 46–51, 2024.

[11] K. Kurdi and J. Cahyono, “Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022,” *JUNCTO J. Ilm. Huk.*, vol. 6, no. 2, pp. 330–339, 2024.

[12] J. E. Widodo, A. Suganda, and T. A. Darodjat, “DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA: DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA,” *PENA LAW Int. J. Law*, vol. 2, no. 2, 2024.

[13] P. R. Saputri, “Perlindungan Privasi Digital dalam Era Digital: Analisis UU No. 19 Tentang Perubahan UU No. 11 Tahun 2008 pada Pemerintahan Joko Widodo,” *Konsensus J. Ilmu Pertahanan, Huk. dan Ilmu Komun.*, vol. 2, no. 2, pp. 112–122, 2025.

[14] E. Asmadi, A. Mansar, and T. Eddy, “Actualization of criminal liability for personal data protection in the use of financial technology: a comparative study of Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 27 of 2022 concerning Protection of Personal Data,” *Lega Lata J. Ilmu Huk.*, vol. 8, no. 2, pp. 292–300, 2023.

[15] N. L. A. Sari, “Penerapan Pasal 28 Ayat (1) Undang-Undang ITE dalam Perspektif Keputusan Bersama Menteri Komunikasi dan Informatika, Jaksa Agung Republik Indonesia dan Kepala Kepolisian Negara Republik Indonesia,” *GANEC SWARA*, vol. 17, no. 1, pp. 124–130, 2023.

[16] M. Mahrina, J. Sasmito, and C. Zonyfar, “The electronic and transactions law (EIT law) as the first cybercrime law in Indonesia: an introduction and its implementation,” *Pena Justisia Media Komun. dan Kaji. Huk.*, vol. 21, no. 2, 2022.

[17] F. Razi and D. P. Markus, “Implementation and Challenges of the Personal Data Protection Law in Indonesia.,” *J. Indones. Sos. Teknol.*, vol. 5, no. 12, 2024.

[18] B. K. Susanto, V. Aprillianto, S. R. Dinni, and F. Nashrillah, “Analisis UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dalam Perspektif Kepentingan Umum: Studi Banding dengan GDPR Uni Eropa, PDPA Singapore, dan DPA Filipina”.

[19] A. Situmeang, N. C. Weley, and H. S. Disemadi, “Kepastian Pertanggungjawaban Hukum Pidana Korporasi atas Penyalahgunaan Data Pribadi di Indonesia,” *Proc. Ser. Soc. Sci. Humanit.*, vol. 23, pp. 8–15, 2025.

[20] A. M. Ar, W. Wirda, A. S. Rusbandi, M. Zulhendra, S. Bahri, and D. Fajri, “Peran Niat (Mens rea) dalam Pertanggungjawaban Pidana di Indonesia,” *Jimmi J. Ilm. Mhs. Multidisiplin*, vol. 1, no. 3, pp. 240–252, 2024.

[21] S. Salsabila and S. A. Wiraguna, “Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia,” *Konsensus J. Ilmu Pertahanan, Huk. dan Ilmu Komun.*, vol. 2, no. 2, pp. 145–157, 2025.

[22] F. M. Rayhan and D. A. Setiawan, "Pertanggungjawaban Pidana terhadap Bjorka sebagai Pelaku Peretas yang Melakukan Kejahatan Pembobolan Data di Indonesia," in *Bandung Conference Series: Law Studies*, 2025, pp. 537–544.

[23] J. A. Halderman, "The Antrim county 2020 election incident: an independent forensic investigation," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 589–605.

[24] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, DC Internet voting system," in *International Conference on Financial Cryptography and Data Security*, Springer, 2012, pp. 114–128.

[25] R. P. Anindya and A. E. Subiyanto, "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 4, no. 3, pp. 1105–1112, 2025.

[26] Z. Cui and Z. Song, "Enterprise Security Incident Analysis and Countermeasures Based on the T-Mobile Data Breach," *arXiv Prepr. arXiv2507.12937*, 2025.

[27] N. M. D. G. Putri and D. G. W. Girinatha, "LEGAL PROTECTION OF PERSONAL DATA OF INDONESIAN CITIZENS BASED ON ACT NUMBER 27 OF 2022," *NOTARIIL J. Kenotariatan*, vol. 9, no. 2, pp. 71–75, 2024.

[28] D. Rusmana, H. Pratikto, and A. Winarno, "Sustainable Tourism Development in Indonesia: A Critical Evaluation of Economic Philosophy," *Enigm. Econ.*, vol. 3, no. 1, pp. 14–26, 2025.

[29] I. P. E. Rusmana, "Kewenangan Antara Bawaslu Dan Aparat Penegak Hukum Dalam Penanganan Tindak Pidana Pemilu," *J. Rechtens*, vol. 13, no. 2, pp. 261–284, 2024.